CLAIMS

1. A computer-implemented method for securely delivering a document from a sender to a recipient, the method comprising an operations center (OC) performing the steps of:

associating the sender with a sender public key from a sender public-private key pair;

using the sender public key, in conjunction with the sender using the sender private key, to authenticate the sender;

establishing a first secure connection between the sender and the OC;

associating the recipient with a recipient public key from a recipient public-private key pair; and

providing one from a group comprising a recipient public key and an escrow encryption key to the sender to secure a delivery, the delivery comprising at least the document.

2. The method of claim 1 further comprising the OC performing the steps of:

receiving at least a portion of the delivery from the sender via the first secure connection;

storing the at least a portion of the delivery;

using the recipient public key, in conjunction with the recipient using the recipient private key, to authenticate the recipient;

establishing a second secure connection between the recipient and the OC; and

transmitting the at least a portion of the delivery to the recipient via the second reliable connection.

3. The method of claim 2 further comprising, in response to the recipient receiving the at least a portion of the delivery, the OC performing one from a group of steps comprising:

notifying the sender to form a secure connection to the recipient to transmit the remainder of the delivery; and

notifying the recipient to form a secure connection to the sender to transmit the remainder of the delivery.

4. The method of claim 3 further comprising the OC performing one from a group of steps comprising:

receiving a first acknowledgement from the sender that the remainder of the delivery was transmitted to the recipient; and

receiving a second acknowledgement from the recipient that the remainder of the delivery was received by the recipient.

5. The method of claim 2 wherein each of the first and second secure connections comprises one from a group comprising a direct line, a virtual private network connection, and a Secure Socket Layer connection.

6. The method of claim 2 wherein at least one of the first and second secure connections comprises a virtual private network connection formed by using a VPN encryption key at a layer selected from a group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnect reference model.

7. The method of claim 2 wherein at least one of the first and second secure connections comprises a virtual private network connection formed by using at least one key from a group comprising the sender public key, the recipient public key, an OC public key, and a session key.

8. The method of claim 3 wherein the secure connection between the sender and the recipient comprises one from a group comprising a direct line, a virtual private network connection, and a Secure Socket Layer connection.

9. The method of claim 3 wherein the secure connection between the sender and the recipient comprises a virtual private network connection formed by using a VPN encryption key at a

layer selected from a group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnect reference model.

10. The method of claim 3 wherein the secure connection comprises a virtual private network connection formed by using at least one key from a group comprising the sender public key, the recipient public key, and a session key.

11. The method of claim 2 wherein the delivery further comprises at least one from the group comprising:

a message digest comprising one of a group of a hash of the document, a hash of the document encrypted with a document encryption key, a hash of the document encrypted with the encryption key, and a hash of the document encrypted with the sender private key from the sender public-private key pair; and

a digital signature signed by the sender private key from the sender public-private key pair.

12. The method of claim 11 further comprising the OC performing the steps of:

storing at least one of the message digest and the digital signature; and

time-stamping and recording an acknowledgement from the recipient that the at least a portion of the delivery was received.

13. The method of claim 2 further comprising the OC performing the step of:

providing a delivery notification to the recipient that the OC is storing the at least a portion of the delivery for the recipient.

14. The method of claim 2 further comprising the OC performing the step of providing a notification to the sender of an event selected from a group comprising:

a failure of the OC to transmit the at least a portion of the delivery to the recipient within a specified time period;

a failure of the OC to locate a valid public key for the recipient;

transmission of the at least a portion of the delivery to the recipient;

receipt of an acknowledgment from the recipient that the at least a portion of the delivery was received;

receipt of an acknowledgment from the recipient that the delivery was received;

receipt of an acknowledgement from the recipient that the document was successfully decrypted; and

a failure of the OC to transmit the at least a portion of the delivery to the recipient because the recipient is unable to access the recipient private key.

15. The method of claim 1 further comprising the OC performing the steps of:

storing the sender public key and the recipient public key in a database; and

providing the sender and the recipient access to the database.

16. The method of claim 15 further comprising the OC performing at least one of the steps of:

revoking the sender public key;

revoking the recipient public key; and

authorizing the generation of a new public-private key pair for at least one of a group comprising the sender, the recipient, and a new user.

17. The method of claim 1 further comprising the OC facilitating a direct and secure connection between the sender and the recipient by the OC performing the steps of:

using the recipient public key, in conjunction with the recipient using the recipient private key, to authenticate the recipient;

receiving a request from the sender to transmit the delivery directly to the recipient; and

providing one from a group comprising:

a notice to the sender that the recipient is available to directly accept the delivery; and

a notice to the recipient that the sender is available to transmit the delivery directly to the recipient.

18. The method of claim 17 further comprising, in response to the sender and the recipient establishing a direct and secure connection and the sender transmitting the delivery to the recipient via the direct and secure connection, the OC performing the steps of:

receiving a sender acknowledgement from the sender that the delivery was transmitted to the recipient; and

receiving a recipient acknowledgement from the recipient that the delivery was received by the recipient.

19. The method of claim 17 wherein the direct and secure connection is a virtual private network connection formed by using a VPN encryption key at a layer selected from a group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnect reference model.

20. The method of claim 17 wherein the direct and secure connection comprises one from a group comprising a direct line, a virtual private network connection, and a Secure Socket Layer connection.

21. The method of claim 17 wherein the direct and secure connection is a virtual private network connection formed by using at least one key from a group comprising the sender public key, the recipient public key, and a session key.

22. The method of claim 17 wherein the delivery further comprises at least one from the group comprising:

a message digest comprising one of a group of a hash of the document, a hash of the document encrypted with a document encryption key, a hash of the document

encrypted with the encryption key, and a hash of the document encrypted with a private key of the sender; and

a digital signature signed by the sender private key from the sender public-private key pair.

23. The method of claim 18 further comprising the OC performing the step of:

time-stamping and recording the sender acknowledgement and the recipient acknowledgement.

24. A system for securely delivering a document from a sender to a recipient, the system comprising an operations center (OC) comprising:

a key manager module for associating the sender with a sender public key from a sender public-private key pair and for associating the recipient with a recipient public key from a recipient public-private key pair;

a directory interface, coupled to the key manager module and to a public key database and an escrow key manager, for searching and returning one key from a group of keys comprising a recipient public key and an escrow encryption key, upon request from the sender for an encryption key;

an authentication module, coupled to the key manager module, for using the sender public key, in conjunction with the sender using the sender private key, to authenticate the sender;

a secure connection module, coupled to the authentication module, for establishing a first secure connection between the sender and the OC;

and

a messaging module, coupled to the secure connection module, for receiving a request from the sender for an encryption key to secure a delivery, the delivery comprising at least the document, and for transmitting to the sender one from a group comprising the recipient public key and the escrow encryption key.

25. The system of claim 24 further comprising:

the authentication module further adapted for using the recipient public key, in conjunction with the recipient using the recipient private key, to authenticate the recipient;

the secure connection module further adapted for establishing a second secure connection between the recipient and the OC;

the messaging module further adapted for receiving at least a portion of the delivery from the sender via the first secure connection and for transmitting the at least a portion of the delivery to the recipient via the second reliable connection; and

a storage area, including a computer-readable medium, coupled to the messaging module, for storing the at least a portion of the delivery.

26. The system of claim 25 further comprising:

the messaging module further adapted for performing, in response to the recipient receiving the at least a portion of the delivery, one from a group of steps comprising:

notifying the sender to form a secure connection to the recipient to transmit the remainder of the delivery; and

notifying the recipient to form a secure connection to the sender to transmit the remainder of the delivery.

27. The system of claim 26 further comprising:

a tracking module, coupled to the messaging module, for receiving a first acknowledgement from the sender that the remainder of the delivery was transmitted to the recipient, and for receiving a second acknowledgement from the recipient that the remainder of the delivery was received by the recipient.

28. The system of claim 25 wherein each of the first and second secure connections comprises one from a group comprising a direct line, a virtual private network connection, and a Secure Socket Layer connection.

29. The system of claim 25 wherein at least one of the first and second secure connections comprises a virtual private network connection formed by using a VPN encryption key at a layer selected from a group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnect reference model.

30. The system of claim 25 wherein at least one of the first and second secure connections comprises a virtual private network connection formed by using at least one key from a group comprising the sender public key, the recipient public key, an OC public key, and a session key.

31. The system of claim 26 wherein the secure connection comprises a virtual private network connection formed by using at least one key from a group comprising the sender public key, the recipient public key, and a session key.

32. The system of claim 25 wherein the delivery further comprises at least one from the group comprising:

a message digest comprising one of a group of a hash of the document, a hash of the document encrypted with a document encryption key, a hash of the document encrypted with the encryption key, and a hash of the document encrypted with the sender private key from the sender public-private key pair; and

a digital signature signed by the sender private key from the sender public-private key pair.

33. The system of claim 32 further comprising:

a tracking module for recording at least one from the group comprising the message digest and the digital signature, and for time-stamping and recording an acknowledgement from the recipient that the at least a portion of the delivery was received.

34. The system of claim 25 further comprising:

the messaging module further adapted for providing a delivery notification to the recipient that the OC is storing the at least a portion of the delivery for the recipient.

35. The system of claim 25 further comprising:

the messaging module further adapted for providing a notification to the sender of an event selected from a group comprising:

a failure of the OC to transmit the at least a portion of the delivery to the recipient within a specified time period;

a failure of the OC to locate a valid public key for the recipient;

transmission of the at least a portion of the delivery to the recipient;

receipt of an acknowledgment from the recipient that the at least a portion of the delivery was received;

receipt of an acknowledgment from the recipient that the delivery was received;

receipt of an acknowledgement from the recipient that the document was successfully decrypted; and

a failure of the OC to transmit the at least a portion of the delivery to the recipient because the recipient is unable to access the recipient private key.

36. The system of claim 24 further comprising:

the key manager module further adapted for providing the sender and the recipient access to the public key database.

37. The system of claim 24 further comprising:

the key manager module further adapted for performing at least one of the steps of:

revoking the sender public key;

revoking the recipient public key; and

authorizing the generation of a new public-private key pair for at least one of a group comprising the sender, the recipient, and a new user.

38. The system of claim 24 further adapted to facilitate a direct and secure connection between the sender and the recipient, the system further comprising:

the authentication module further adapted for using the recipient public key, in conjunction with the recipient using the recipient private key, to authenticate the recipient;

the messaging module further adapted for receiving a request from the sender to transmit the delivery directly to the recipient, and for providing one from a group comprising:

a notice to the sender that the recipient is available to directly accept the delivery; and

a notice to the recipient that the sender is available to transmit the delivery directly to the recipient.

39. The system of claim 38 further comprising:

the messaging module further adapted for receiving, in response to the sender and the recipient establishing a direct and secure connection and the sender transmitting the delivery to the recipient via the direct and secure connection:

a sender acknowledgement from the sender that the delivery was transmitted to the recipient; and

a recipient acknowledgement from the recipient that the delivery was received by the recipient.

40. The system of claim 38 wherein the direct and secure connection comprises a virtual private network connection formed by using a VPN encryption key at a layer from a group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnect reference model.

41. The system of claim 38 wherein the direct and secure connection comprises one from a group comprising a direct line, a virtual private network connection, and a Secure Socket Layer connection.

42. The system of claim 38 wherein the direct and secure connection comprises a virtual private network connection formed by using at least one key from a group comprising the sender public key, the recipient public key, and a session key.

43. The system of claim 38 wherein the delivery further comprises at least one from the group comprising:

a message digest comprising one of a group of a hash of the document, a hash of the document encrypted with a document encryption key, a hash of the document encrypted with the encryption key, and a hash of the document encrypted with a private key of the sender; and

a digital signature signed by the sender private key from the sender public-private key pair.

44. The system of claim 39 further comprising:

a tracking module for time-stamping and recording the sender acknowledgement and the recipient acknowledgement.

45. In a computer-readable medium, a computer program product for an operations center (OC) facilitating secure delivery of a document from a sender to a recipient, the computer-readable medium comprising program code adapted to perform the steps of:

associating the sender with a sender public key from a sender public-private key pair;

using the sender public key, in conjunction with the sender using the sender private key, to authenticate the sender;

establishing a first secure connection between the sender and the OC;

associating the recipient with a recipient public key from a recipient public-private key pair; and

providing one from a group comprising a recipient public key and an escrow encryption key to the sender to secure a delivery, the delivery comprising at least the document.

46. The computer readable medium of claim 45 further comprising program code adapted to perform the steps of:

receiving at least a portion of the delivery from the sender via the first secure connection;

storing the at least a portion of the delivery;

using the recipient public key, in conjunction with the recipient using the recipient private key, to authenticate the recipient;

establishing a second secure connection between the recipient and the OC; and

transmitting the at least a portion of the delivery to the recipient via the second reliable connection.

47. The computer readable medium of claim 46 further comprising program code adapted to perform, in response to the recipient receiving the at least a portion of the delivery, one from a group of steps comprising:

notifying the sender to form a secure connection to the recipient to transmit the remainder of the delivery; and

notifying the recipient to form a secure connection to the sender to transmit the remainder of the delivery.

48. The computer readable medium of claim 47 further comprising program code adapted to perform one from a group of steps comprising:

receiving a first acknowledgement from the sender that the remainder of the delivery was transmitted to the recipient; and

receiving a second acknowledgement from the recipient that the remainder of the delivery was received by the recipient.

49. The computer readable medium of claim 46 wherein each of the first and second secure connections comprises one from a group comprising a direct line, a virtual private network connection, and a Secure Socket Layer connection.

50. The computer readable medium of claim 46 wherein at least one of the first and second secure connections comprises a virtual private network connection formed by using a VPN encryption key at a layer selected from a group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnect reference model.

51. The computer readable medium of claim 46 wherein at least one of the first and second connections comprises a virtual private network connection formed by using at least one key from a group comprising the sender public key, the recipient public key, an OC public key, and a session key.

52. The computer readable medium of claim 47 wherein the secure connection between the sender and the recipient comprises one from a group comprising a direct line, a virtual private network connection, and a Secure Socket Layer connection.

53. The computer readable medium of claim 47 wherein the secure connection between the sender and the recipient comprises a virtual private network connection formed by using a VPN encryption key at a layer selected from a group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnect reference model.

54. The computer readable medium of claim 47 wherein the secure connection comprises a virtual private network connection formed by using at least one key from a group comprising the sender public key, the recipient public key, and a session key.

55. The computer readable medium of claim 46 wherein the delivery further comprises at least one from the group comprising:

a message digest comprising one of a group of a hash of the document, a hash of the document encrypted with a document encryption key, a hash of the document encrypted with the encryption key, and a hash of the document encrypted with the sender private key from the sender public-private key pair; and

a digital signature signed by the sender private key from the sender public-private key pair.

56. The computer readable medium of claim 55 further comprising program code adapted to perform the steps of:

storing at least one of the message digest and the digital signature; and

time-stamping and recording an acknowledgement from the recipient that the at least a portion of the delivery was received.

57. The computer readable medium of claim 46 further comprising program code adapted to perform the step of:

providing a delivery notification to the recipient that the OC is storing the at least a portion of the delivery for the recipient.

58. The computer readable medium of claim 46 further comprising program code adapted to perform the step of providing a notification to the sender of an event selected from a group comprising:

a failure of the OC to transmit the at least a portion of the delivery to the recipient within a specified time period;

a failure of the OC to locate a valid public key for the recipient;

transmission of the at least a portion of the delivery to the recipient;

receipt of an acknowledgment from the recipient that the at least a portion of the delivery was received;

receipt of an acknowledgment from the recipient that the delivery was received;

receipt of an acknowledgement from the recipient that the document was successfully decrypted; and

a failure of the OC to transmit the at least a portion of the delivery to the recipient because the recipient is unable to access the recipient private key.

59. The computer readable medium of claim 45 further comprising program code adapted to perform the steps of:

storing the sender public key and the recipient public key in a database; and

providing the sender and the recipient access to the database.

60. The computer readable medium of claim 59 further comprising program code adapted to perform at least one of the steps of:

revoking the sender public key;

revoking the recipient public key; and

authorizing the generation of a new public-private key pair for at least one of a group comprising the sender, the recipient, and a new user.

61. The computer readable medium of claim 45 further comprising program code adapted to facilitate a direct and secure connection between the sender and the recipient by performing the steps of:

using the recipient public key, in conjunction with the recipient using the recipient private key, to authenticate the recipient;

receiving a request from the sender to transmit the deliver directly to the recipient; and

providing one from a group comprising:

a notice to the sender that the recipient is available to directly accept the delivery; and

a notice to the recipient that the sender is available to transmit the delivery directly to the recipient.

62. The computer readable medium of claim 61 further comprising program code adapted to perform the steps of:

in response to the sender and the recipient establishing a direct and secure connection and the sender transmitting the delivery to the recipient via the direct and secure connection:

receiving a sender acknowledgement from the sender that the delivery was transmitted to the recipient; and

receiving a recipient acknowledgement from the recipient that the delivery was received by the recipient.

63. The computer readable medium of claim 61 wherein the direct and secure connection comprises a virtual private network connection formed by using a VPN encryption key at a layer selected from a group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnect reference model.

64. The computer readable medium of claim 61 wherein the direct and secure connection comprises one from a group comprising a direct line, a virtual private network connection, and a Secure Socket Layer connection.

65. The computer readable medium of claim 64 wherein the direct and secure connection comprises a virtual private network connection formed by using at least one key from a group comprising the sender public key, the recipient public key, and a session key.

66. The computer readable medium of claim 61 wherein the delivery further comprises at least one from the group comprising:

a message digest comprising one of a group of a hash of the document, a hash of the document encrypted with a document encryption key, a hash of the document encrypted with the encryption key, and a hash of the document encrypted with a private key of the sender; and

a digital signature signed by the sender private key from the sender public-private key pair.

67. The computer readable medium of claim 62 further comprising program code adapted to perform the step of:

time-stamping and recording the sender acknowledgement and the recipient acknowledgement.